How to Setup Pen Testing Lab

By
Anant Shrivastava
http://anantshri.info

What is a Pen test Lab

- A Pen testing Lab just like any other lab is a controlled environment where behavioral or operational patterns of a object / application could be studied for enhancement of skill / knowledge of the practitioner.

- More specifically we try to create a replica of Wild Wild West and try to study it in a controlled manner

Why

- Give me six hours to chop down a tree and I will spend the first four sharpening the axe.

  -Abraham Lincoln
- Practice enhances perfection
- Do I need to say more…..

What we will be practicing

- A pentest lab could be a generalized lab or focused lab towards one single approach.
- Such as
  - network testing
  - web app testing
  - malware analysis
  - mobile analysis
  - More and more…

Standards good to know

- OWASP – Open Web Application Security Project
- OSSTMM - Open Source Security Testing Methodology Manual
- ISO 27001 – auditing standard : (protection mechanism postmortem details).

Lets Get Started

- What are the basic requirements of a Pentest Lab.
- Network
- 2-3 PC
- Some vulnerable stuff.
- Some toolset.
- And of course a Twisted mind ☺

Approach 1

- Purchase a Switch/Router
- Keep two powerful computers make one as target another as attacker.
- PC target : could be loaded with prebuilt vulnerable software stacks. (examples ahead)
- PC attack : load it with self build tool chain or prebuilt tool chain.

Approach 2

- Virtualization
- 1 Powerful Laptop / Desktop (>=4GB RAM, 64bit, 2.4+ preferable Quad Core)
- Virtualization Solution
  - VMWare
  - Oracle ~~Sun Innotek~~ Virtual BOX
  - ☺ Microsoft virtual PC ☺
- Minimum 2 VM
  - Target
  - Attacker

Attack Machine

- Again Self Created or
  - Backtrack
  - Matriux
  - Moth/Lambert
  - Helix(Forensic Distro)
  - SIFT
  - Lots more google is your friend
- I prefer Keeping a windows VM also and load tools specific to windows inside the VM

Target Machine

- Target Machine, either we can prepare ourself or use existing prebuilt images like
  - MetaSploitable
  - Unpatched Windows 2000, Xp
  - Damn Vulnerable Linux
  - de-ice
  - Hackerdemia
  - pWnOS
  - Ubuntu 7.04

Web Application testing

- For Web applications You need some vulnerable Web application code
  - WebGoat
  - Hacme Tools(bank, Casion,Books,Travel…)
  - Damm vulnerable app
  - http://demo.testfire.net/
  - http://testasp.acunetix.com/
- Or Download old version of joomla, wordpress, drupal set it up and you are good to go..

Do’s and Don’t

- Avoid using main machine for any analysis.
- Avoid Giving Read write access to VM over any folder of parent. (specially if VM and main OS are same)
- Once your VM is prepared keep a screnshot. And you can use it as restore point after every session to get back to clean state.

Network Testing

- For Network Testing you could look at GNS3 for setting up the environment. (ciso/juniper routers / switches)
- Would recommend : http://www.gns3.net/content/gns3-virtualbox-edition
- Excellent guides are already available online
- http://www.gns3.net/documentation

Part 1 Over

- However Does it satisfies your hunger?
- Do you feel like conquering something even if you get inside one of the machine.
- Initially yes but later NO.

- It fails to satisfy the fun of manhandling the live target.
- So lets see If we have any option of doing it within legal limits.

Beyond just Lab

1. We can practice of online playgrounds.
   - Live websites providing new challenges every now and then.
     1. Honeynet.org
     2. Hackthissite.org
     3. Smashthestack.org
     4. Intruded.net
     5. internot
     6. http://projectshellcode.com/
     7. For casual brain teasing Check hacker.org

     Are just a few examples

Beyond just lab

- Practice on Live target’s willing to pay
  - Facebook.com
  - Mozilla for its products
  - Google.com

Note : Do read the SOW and then only start.

Capture The Flag

- You can also participate in various CTF competition. (result fame and / or money besides increase in knowledge and confidence)
- Capture the flag or CTF are competitions organized world wide in both online and offline mode.
- People either team up and play against computer / organizer or are pitted against each other.

Online CTF

- When players play against organizer, they are given set of challenges which they need to complete within stipulated time limit and max scorer wins.
- Some common characteristics
  - The challenges will try to touch all bases of ethical hacking (web app, RE, forensics, crypto and more)
  - You can keep your Zero days with you.
  - Generally challenges will be checking your approach and not how quickly you can skim through osvdb or exploit-db
  - Nearly 100% require documented approach to be a winner.

Must have tools

- These are tools and command that have made by must know how to use and must be ready to be used list
  - Ping, ssh, telnet, scp, mount, fsck, file
  - Nmap, gdb
  - Strace, ltrace, ptrace
  - Strings, Hexedit
  - Wireshark, aircrack suite
  - Firefox plugin set : tamper data, live header, firebug etc.
  - Windows tools : Network Miner (this tool alone is my reason as of now to keep a windows VM)
  - Metasploit, burp/ZAP.

NOTE : YMMV : your mileage may vary

One on One

- This type of CTF is generally played in offline mode.
- Each team is given a machine to play.
- Machine contains a flag.
- Task is to save your flag and also capture opponents flag.

- This is Wild Wild West keep aside all books and start shooting as much arsenal as you have.
- Good approach is to have few members focusing on hardening and others focusing on attack.
- These events do see lots and lots of DDoS and DoS attacks

Resources to follow

- BackTrack Mailing list
- Full Disclosure (select mailing list of interest)
  - Main full disclosure
  - Web application security
- Security focus (select mailing list of interest)
  - Security basics
- **SANS Internet Storm Center**
- **Darknet**
- To name a few

THANK YOU

Anant Shrivastava

http://anantshri.info